CHAPTER 2

TEORI AND REVIEW

2.1 Literature Study

In this literature study section, it is a part to find thesis writing materials that are relevant to topics that can be obtained from books, journals and websites related to Internet of Things (IoT) Data Security Using AES Algorithm. The journals in this literature study will be a reference for writers for thesis writing so that authors have innovation and know the limitations of what has been done in the reference journal.

Here are some studies that have been done to overcome this Internet of Things (IoT) Data Security problem. Several summaries of the Literature Study are used to determine the extent to which the research has been carried out.

Table 2.1 Literature Study

NO	Title & Year	Author's Name	Methods (Issues are raised)	Research Limits
1.	Low-Power AES Data Encryption Architecture for a LoRaWAN. (2019).	Tsai, KunLin Leu, FangYie You, Ilsun Chang, ShuoWen Hu, ShiungJie Park,Hoonyong .	The research discusses about LoRaWAN developed by the LoRa Alliance, which is a suitable long-distance wide area network specification for the IoT environment because of its low-power communications. uses three	Research is focusing on reducing the consumption of power atthe time of doing the encryption and also reduce the occurrence of delays the process of encryption / decryption [7].

			communication modes to further reduce power consumption and uses Advanced Encryption Standard (AES) cryptography to improve it network security [7].	
2.	Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices. (2016).	Ometov, Aleksandr Masek, Pavel Malina, Lukas Florea, Roman Hosek, Jiri Andreev,Sergey Hajny, Jan Niutanen, Jussi Koucheryavy, Yevgeni.	This study aims to provide a study of the application of state-of-the-art cryptographic primitives for IoT devices, including pair based cryptography. Symmetric cryptography is widely recognized as the basis for many advanced cryptography, such as privacy protection and identity based encryption [8].	This research only focuses on what devices are suitable for certain cryptographic operations [8].
3.	An Efficient Collision	Niu, Yongchuan	The purpose of this study is to propose	This study focuses on three typical

	Power Attack on AES Encryption in Edge Computing. (2019).	Zhang, Jiawei Wang, An Chen, Caisen.	a new type of Collision attack by exploiting leaks of a linear layer, which is able to solve the masking scheme with uniformly distributed random masks [9].	implementations of AES in Edge computing, and proposes a new type of Collision by exploiting leaks from linear layers [9].
4.	Comprehensive Analysis on the SecurityThreats and their Counterme asures of IoT. (2017)	Wahab, Abdul Ahmad, Omair Muhammad, Mian Ali, Munam.	This study aims to discuss the security of the 4 layer IoT architecture. Where each layer has different security features such as cryptography, sensor data protection, communication security etc [10].	This study only discusses security vulnerabilities at various layers of IoT, without presenting preventive measures against security threats, preventing any damage to the IoT network and the steps that should be taken to ensure the security and privacy of IoT users [10].

This study will use the AES algorithm as a proposed security method on Internet of Things data contained in the database server. This study also uses AES 128, where AES 128 uses 10 repetitions to perform the encryption process [5]. AES 128 is suitable for encrypting data because it has a shorter processing time compared to AES 192 and AES 256. AES 128 also has a good level of security [25].

2.2 Basic Theory

2.2.1 Definition of the Internet of Things (IoT)

In line large Internet of things is a concept or program that has the ability to transmit or send the data through the network without using a support device computers and humans . Internet of things, or often referred to IOT when it experienced a lot of growth . The development of IoT can be seen starting from the convergence level of wireless technology, microelectromechanical (MEMS), internet, and QR (Quick Responses) Code [11] . IoT is also often identified with RFID (Radio Frequency Identification) as a method of communication [1] .

IoT consists of 4 layers, namely the physical layer, network layer, processing layer, and application layer. Physical layer tasked to collect all the data obtained from sensors and devices physically more [10]. Layer is also held responsible for the communication between devices. Layer the second is the network layer where the layer is held responsible for communication between devices physically are different, management of the network and also for the maintenance of information through many communication protocols in the system IOT [24]. The third layer is the processing layer, this layer functions to combine the network layer and the physical layer [10].

Due to the large amount of data , it is very important to store and process data using storage databases. Efforts security in layers this is a Web application scanners. The last layer is the application layer where the layer is a layer oriented services that provide context-aware services between devices that connect [10].

IoT can be categorized as a very complex system and is also vulnerable to cyber attacks [19]. All IoT layers are vulnerable to attack, especially at the sensor layer [10]. These devices are connected via a public network or the internet, so that the perpetrators of the attack can attack them using certain techniques. One of the only issues the attack that flare occurs namely Data & Identity Theft, here the perpetrator stole data while sent from the device

to the to the data server and vice versa [22]. The perpetrator can read data that has been stolen because the data has not been secured before being sent [22].

2.2.2 Data on IoT Devices

In general, data can be interpreted as a record of a collection of facts. Data is a form of plural of datum, derived from the language of Latin that means "something that is given" [20]. In everyday use, data means a statement that is accepted for what it is. Statement This is the result of the measurement or observation of a variable whose shape can be numbers, words, or images [20]. But what is meant by data on the Internet of Things, is an input sourced from a sensor which will then be sent to a web server storage media and will be an output or output [21].

Data on the Internet of Things is highly vulnerable to all kinds of attacks. Without the security of data on the Internet of Things of course can lead to a risk that the information is sensitive and valuable can be in access by people who do not shall responsibilities [12]. In addition to the data that was hacked possibility would be damaged or lost in which case it may cause damage to the system IOT. By because it is the security of data on the Internetof Things is required [12].

2.2.3 Cryptographic Definitions

Cryptography is the science that studied the techniques of mathematics that relates to the aspect of security information such as confidentiality, integrity of data, and authentication [23]. To be able to run the cryptographic process properly there must be four main elements, where these elements are interrelated with each other. That is :

- Plain Text is a message beginning or message the original that send to the process of communication . Plain Text is this which then in encryption and in the description [12].
- Cipher Text merupaka message that is hidden , that is a message

the original (Pain Text) which has been in encryption Dapa process of cryptography . Cipher Text this can be changed back to forms the original (Pain Text) utilizing Key that has been in providing [12].

- Cryptography Key is a key that is used to perform encryption and descriptions in the cryptographic process . Without the key (key) that is equal then the process of encryption and description tidaka can be done with either . Key (key) is information that is solid into the control of the process of the cryptographic [12].
- Encryption Decryption Algorithm is an algorithm that is used for encryption and decryption [12].

2.2.4 AES Algorithm

Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to synchronize data. The AES algorithm is a symmetric ciphertext block that can encrypt (encipher) and decrypt (decipher) information [3]. Encryption changes data that can no longer be read called ciphertext, conversely, decryption is changing the ciphertext data into its original form which we know as plaintext. The AES algorithm uses cryptographic keys 128,192, and 256 bits to encrypt and decrypt data.

Advanced Encryption Standard (Standard Encryption Advanced) is one of the methods most commonly to encrypt the data is important, which has been used by organizations large world such as Apple and Microsoft to NSA [18]. The algorithm AES has the ability to defend against an attack far more better than the method of encryption other. The AES algorithm is efficient on a computer and memory basis as well as more flexibility and is particularly suitable whenapplied to both hardware and software.

On the whole, AES consists of three encoding blocks namely AES-128, AES-192 and AES-256 [13]. Each AES encoding encrypts and decrypts data in 128-bit blocks using cryptographic keys for 128, 192 and 256-bits with 256-bit being the most secure. For 128-bit keys, there are 10 rounds of the encryption process, 12 rounds for the 192-bit key and 14 rounds for the 256-bit key [13]. The algorithm AES was symmetrical, meaning that when the keys are the same used for the process of encryption and decryption, so the sender and receiver know when they use a key that is the same.

2.2.5 Symmetric Cryptography on IoT Devices

The IoT devices discussed in this study focus more on microcontroller devices. Generally, the data is sent from the microcontroller to the server is still shaped plaintext, meaning that the data that they can be read by anyone alone. The method of encryption can be used for securing the data are. Method of encryption that is appropriate to use that method of encryption symmetric, because the method is more rapid and efficient use of memory

compared to the method of encryption asymmetric [14]. Algorithm encryption symmetric who used that algorithm AES.

2.3 IoT Device Prototype

This study will use one of the IoT devices, namely the ultrasonic sensor HCSR04 where this sensor is used to measure the distance from an object, the range of distance that can be measured is about 2 - 450 cm. This tool uses NodeMcu as its microcontroller. The following hardware and software are used:

2.3.1 NodeMCU

NodeMCU is an IoT platform which is opensource [15]. Consists of device hardware such as System On Chip ESP8266 of ESP8266 artificial Espressif System, also the firmware that uses language programming Lua scripting. Theterm NodeMCU by default actually refers to the firmware that use of the device hardware development kit. NodeMCU can be analogized as a board arduino its ESP8266. NodeMCU have me-package ESP8266 into in a board that is compact with various features like microcontrollers + capability of access to Wifi also chip communication USB to serial [15]. So to program it only requires the exact USB data cable extension that is used as the data cable and charging cable for the Android smartphone. NodeMCU basic specifications :

- Microcontroller: Tensilica 32 bit
- Flash Memory: 4 KB
- Operating Voltage : 3.3 V
- Input voltage : 7 - 12 V
- Digital I / O: 16
- Analog Input: 1 (10 Bit)
- UART interface : 1
- SPI Interface : 1
- Interface I2 C: 1

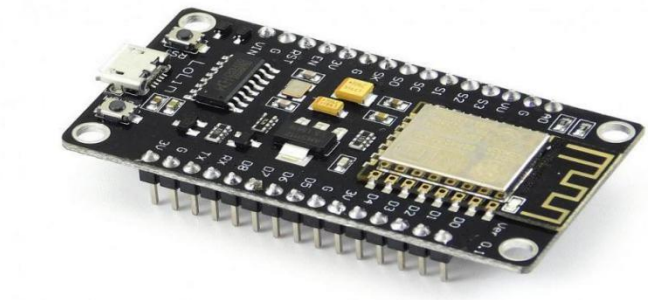

Figure 2. 1 NodeMCU

The ESP8266 uses the JEDEC standard voltage (3.3V voltage). Unlike AVR microcontrollers and most Arduino boards that have a TTL voltage of 5 volts. Even so, the mcu node can still be connected to 5V but via the micro USB port or Vin pin provided by the board. However, all pins on the ESP8266 are intolerant of 5V input. So don't immediately paint it with TTL voltage if you don't want to damage your board. You can use the Level Logic Converter to convert the voltage to a safe value of 3.3v.

2.3.2 HC-SR04 Sensor

The ultrasonic sensor HCSR04 is a device used to measure the distance from an object. The range of the measurable distance is about 2 - 450 cm. This device uses two digital pins to communicate the read distance [16]. The working principle of this ultrasonic sensor works by sending an ultrasonic pulse of about 40 KHz, then it can reflect the echo pulse back, and calculate the time taken in microseconds [16].

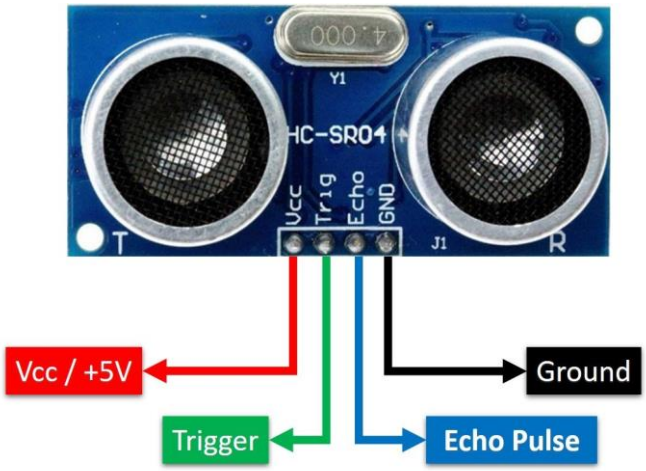

Figure 2.2 HC-SR04 Sensor

2.3.3 Power Supply

Power Supply is an electrical device that can provide electrical energy for other electrical or electronic devices [17]. Basically, this power supply requires a source of electrical energy which then converts it into electrical energy needed by other electronic devices. Therefore, the Power Supply is sometimes also referred to as the Electric Power Converter.